Examination of Some Foremost Security Concerns of Contemporary Cloud Computing Environments

Reshma Ashik Chauhan

Senior Research Analyst, SMRVD Security Solutions, India.

Abstract: Cloud computing diminishes cost and complexity of service providers by means of assets and operational costs. It allows users to access applications tenuously. On behalf of user, this construct directs cloud service provider to feel software updates and cost of servers etc. For cloud providers and consumers; availability, integrity, authenticity, confidentiality, and privacy are important concern. Infrastructure as a Service (IaaS) serves as base layer for many other release models and Platform-as-a-Service (PaaS) clouds. In this paper we are going to some major security issues of current cloud computing environments. Security of PaaS clouds is considered from multiple perspective including access control, service continuity and privacy while protecting together the service provider and the user. Security problems of PaaS clouds are explored and classified.

Keywords: Cloud Computing; Security; Issues.

1. Introduction

Existing security-based solutions, including authentication and cryptography-based solutions, provide security resolutions to a certain extent and cannot tackle various internal attacks. Mostly in academia, more emphasis is being put on the implementation of security frameworks in edge-based smart cities. The basic concept behind the edge computing networks is to utilize a hierarchy of edge network-based servers with increased computational capabilities to handle the mobile and heterogeneous computational tasks typically offloaded by low-end edge devices (IoT and mobile devices) [1-11]. Edge computing can support evolving smart city applications by providing location-aware, bandwidth-sufficient, real-time, privacy-conscious, and low-cost services. Edge computing has grown rapidly in recent years as a result of its advantages over CC. Providing by cloud infrastructure providers, data owners outsource gradually data to the data centers concluded cloud service providers, e.g., the online storage facility providers, which are not completely trusted by data owners.

To define the relation between entities, the graph has been increasingly used to model complicated organizations and schema less data, such as the personal social network (the

social graph), the relational data base, Considered for the protection of users' privacy. These sensitive data have to be encrypted before outsourcing to the cloud. Furthermore, nearly data are invented to be shared among trusted partners to all organizations [12-26]. There have stayed revealed attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to illuminate before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, faults, analyzes the profits and cloud computing information security management.

There are several major cloud computing providers with Amazon, Salesforce, Google, Yahoo, Microsoft and others that are providing cloud computing services [27-34]. Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, infrastructure-as-a-services, software-as-a-services etc. The attractiveness of cloud computing is not only to large enterprises but also startups, entrepreneurs, medium companies and small companies would benefit greatly and they will have a opportunities and alternative that is not available to them in the past that would save them billions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, communication capacity and storage space from a large cloud computing provider that has all of these assets connected towards the Internet [35-42]. In practice, cloud service providers tend to offer services that can be grouped into three categories: infrastructure as a service, platform as a service, and software as a service.

Figure 1. Software as a Service (SaaS) (Source: Internet)

If provide software services on demand. The use of single occurrence of the application runs on the cloud services and multiple end users or client organizations. The

most usually known example of SaaS is salesforce.com, though many other examples have revive market, including the Google Apps offering of basic corporate services including email and word processing. Even though salesforce.com led the definition of cloud computing by a limited years, it now operates by leveraging its companion force.com, which can be demarcated by way of a platform as a service.

Platform as a service condenses a layer of software and make available it as a service that can be used to build higher level services. There are at least two perspectives on PaaS provisional on the perspective of the producer or consumer of the services: Someone producing PaaS potency produce a platform by participating an OS, middleware, application software, and even a development environment that is before provided to a customer as a service [43-55]. Someone using PaaS would see an summarized service that is presented to them through an API. The customer interacts by the platform through the API, before the platform does what is necessary to manage and scale itself to provide a specified level of service. Virtual appliances can be hush-hush as instances of PaaS. A content switch appliance, for example, would have all of its component software unseen from the customer, and only an API or GUI for configuring and deploying the service provided to them. PaaS assistances can provide for every phase of software development and testing, or they can be specialized everywhere a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which assists applications on Google's infrastructure. PaaS services such as these can provide a powerful origin on which to deploy applications, however they may be forced by the capabilities that the cloud provider indicates to convey.

Infrastructure as a service delivers basic storage and compute capabilities as consistent services over the network. Servers, storage systems, switches, routers, and other systems are united and made available to holder workloads that range from application components to high performance computing applications. Commercial samples of IaaS include Joyent, whose main product is a line of virtualized servers that afford a highly available on demand infrastructure.

2. Attacks in Cloud Computing

Cloud computing faces just as much security threats that are at present found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk susceptibilities come in many forms. The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats roughcast cloud computing and it identified the

flowing major threats:

- Shared Technology Vulnerabilities
- Failures in Provider Security
- Availability and Reliability Issues
- Integrating Provider and Customer SecuritySystems
- Legal and Regulatory Issues
- Insecure Application Programming Interfaces
- Perimeter Security Model Broken
- Data Loss/Leakage
- Malicious Insiders

With the security risk and susceptibility in the enterprise cloud computing that are being exposed enterprises that want to ensue with cloud computing should, use the following steps to substantiate and understand cloud security providing by a cloud provider: Understand: the cloud by appreciating how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by consuming an in-depth understanding of how cloud computing transmit and handles data.

Demand Transparency: by constructing sure that the cloud provider can hoard detailed information on its security architecture and is agreeable to accept regular security audit. The regular security appraisal should be from an independentbody or centralized agency.

Reinforce Internal Security: by making sure that the cloud provider's internal security technologies and practices with firewalls and user access controls are very strong and can lattice very well through the cloud security measures.

Contemplate the Legal Implications: by significant how thelaws and regulations will affect what you lead into the cloud. Pay attention: by constantly observing any development orchanges in the cloud technologies and practices that mayimpression your data's security.

3. Implementing Cloud Computing

The world's important information technology, advisory company, research and has identified seven security apprehensions that an enterprise cloud computing user should discourse with cloud computing providers before approving.

Regulatory Compliance: Create sure your provider is willing to submit to external Audits and security certifications.

User Access. Ask providers for unambiguous information on the hiring and oversight of privileged administrators and the controls concluded their access to information. Major Companies should demand and enforce their own hiring principles for personnel that will operate their cloud computing environments.

Data Segregation: Realize what is done to segregate your data, and probe for proof that encryption schemes are deployed and are effective.

Data location: Enterprises should necessitate that the cloud computing provider store and process data in specific jurisdictions and should follow the privacy rules of those Jurisdictions.

Disaster Recovery Ask the provider for a contractual commitment to sustenance specific types of investigations, such as the research involved in the discovery phase of litigation, and verifies that the provider has successfully supported such activities in the past. Deprived of evidence, don't assume that it can do so.

Disaster Recovery Verification Know what will happen if adversity strikes by asking whether your provider will be capable of utterly restore your data and service, and find out how long it will take.

Long-term Viability: Ask forthcoming providers how you would get your data back if they were to fail or be assimilated, and find out if the data would be in a arrangement that you could easily import into a replacement application.

4. Solutions

First solution is of verdict the right cloud provider. Different vendors have dissimilar cloud IT security and data management. A cloud vendor should be well established, have experience, principles and regulation. So there is not some chance of cloud vendor closing.

Contract with cloud vendor should be clear. So if cloud vendor closes earlier contract, enterprise can claim.

Cloud vendors ought to provide very good recovery facilities. So, if data are fragmented or lost because of certain issues, they can be recovered and continuity of data can be managed.

Enterprise requisite have infrastructure which enables installation and configuration of hardware components such as firewalls, routers, software, servers and proxy servers such as operating system, thin clients, etc. Similarly ought to have infrastructure which prevents from cyber-attacks.

Developers should develop the solicitation which provides encrypted data for the security. So further security from enterprise is not crucial and all security burdens are placed on cloud vendor. IT leaders must define approach and key security components to know where the data encryption is needed.

There should be a chart apropos the tide of data. So the IT managers can have idea where the data is on behalf of all the times, where it is being stored and where it is being united. There should be total exploration of data.

5. Conclusions

Services are to be offered by providers, to consumers with proper SLAs. Basic entities of crypto-cloud have the responsibility of maintaining the SLAs. Resource provisioning at any time depends on the bandwidth required, CPU, memory and key management amongst others. Different levels of SLA's exist and they are customer-based, service-based and multi-level SLA. Although Cloud computing can be seen as a new marvel which is set to reform the way we use the Internet, there is much to be thoughtful about. There are many new technologies emerging at an express rate, each with technological developments and with the potential of making human’s lives at ease. However, one must be very careful to appreciate the security risks and challenges stood in exploiting these technologies. Cloud computing is no exception. In this paper Security issues in Service Model of cloud computing Environment which are currently handled in the Cloud computing are highlighted. Cloud computing has the possible to become a favorites in stimulating a secure, virtual and economically possible IT solution in the forthcoming.

References

[1] Laniepce S, Lacoste M, Kassi-Lahlou M, Bignon F, Lazri K, Wailly A. Engineering intrusion prevention services for IaaS clouds: the way of the hypervisor, 2013 IEEE seventh international symposium on service-oriented system engineering.

[2] Vyas J. Prof: Prashant Modi, `providing confidentiality and integrity on data stored in cloud storage by hash and meta-data approach. Int J Adv Res Eng, Sci. Technol. May 2017;4(5). e-ISSN: 2393-9877, p-ISSN: 2394-2444.

[3] Chatterjee R, Roy S. Cryptography in cloud computing: a basic approach to ensure security in cloud. IJESC 2017;7(5).

[4] Bhargav Vora S, Anandache JG. Data Backup on: cloud computing Techniques in digital libraries perspective. J Global Res Comput Sci May 2015.

[5] Vinod Varma Vegesna (2023). “Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads,” International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[6] Vinod Varma Vegesna (2022). “Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues,” International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[7] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[8] Hamid Ali Abed Al-Asadi and et al., “Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network”, Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[9] Hamid Ali Abed Al-Asadi and et al., “A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[10] Vinod Varma Vegesna (2022). “Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions,” Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[11] Negi T, Chaudhary S, Rautela S. Data security in cloud computing. Int J Adv Res Comput Sci Software Eng May 2015;5(5) ISSN: 2277 128X.

[12] Sabahi F. Secure virtualization for cloud environment using hypervisor-based technology. Int J Mach Learn Comput February 2012;2(1).

[13] Kamara S, Lauter K. Cryptographic cloud storage. Microsoft Research Cryptography Group; January 2010 http://research.microsoft.com/pubs/112576/cryptocloud.pdf.

[14] Rebollo O, Mellado D, Fernandez-Medina E, Mouratidis H. Empirical evaluation of a cloud computing information security governance framework. Inf Software Technol 2015;58:44–57.

[15] Bhadauria R, Sanyal S. Survey on security issues in Cloud Computing and Associated Mitigation Techniques. Int J Comput Appl (0975-888) June 2012;47(18).

[16] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[17] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications,” International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[18] Hamid Ali Abed Al-Asadi, et al., “Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement”, Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[19] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[20] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[21] Vinod Varma Vegesna (2022). “Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems,” Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[22] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[23] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[24] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at

SSRN: https://ssrn.com/abstract=4418127

[25] Kaur S, Khurmi DS. A review on security issues in cloud computing. Int J Comput Sci Technol March 2016.

[26] Vinod Varma Vegesna (2021). "A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments," International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[27] Vinod Varma Vegesna (2021). "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing," International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[28] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[29] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[30] Vinod Varma Vegesna (2021). "The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes," International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[31] Vinod Varma Vegesna (2020). "Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications," Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[32] Asghar MR, Ion M, Russello G. Bruno Crispo2. Securing data provenance in the cloud, conference paper. January 2011.

[33] Bose R, Sarddar D. A SecureHypervisor-based technology create a secure cloud environment. Int J Emerg Res Manage Technol February 2015;4(2). ISSN: 2278-9359.

[34] Nawaz Brohi S, Adib Bamiah M, Nawaz Brohi M, Kamran R. Identifying and analyzing security threats to virtualized cloud computing infrastructures, In Proceedings of 2012 international of cloud computing, technologies, applications and management.

[35] Zhang S. Deep-diving into an easily- overlooked threat: inter-VM attacks. http://people.cis.ksu.edu/~zhangs84/papers/cloudTR.pdf; 2012.

[36] More A, Tapaswi S. Virtual machine introspection: towards bridging the semantic gap. J Cloud Comput Dec 2014.

[37] Vinod Varma Vegesna (2019). "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[38] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[39] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[40] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[41] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci 2014;258:371–86.

[42] Qin Z, Zhang Q, Wan C, Di Y. State-of-the-art virtualization security in cloud computing. J Inf Comput Sci 2012;9(6):1487–97.

[43] Dongxi L. A cloud architecture of virtual trusted platform module, Embedded and Ubiquitous Computing (EUC). IEEE/IFIP 8th International conference on. vol.2010.

[44] Mathisen E. Security challenges and solutions in cloud computing. On 5th IEEE International conference on digital ecosystems and technologies (IEEE DEST 2011). 2011.

[45] Turnbull L, Shropshire J. Breakpoints: an analysis of potential hypervisor attack vectors. IEEE; 2013.

[46] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[47] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[48] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, "Fuzzy Logic approach to Recognition of Isolated Arabic Characters",

International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[49] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, “Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers,” Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[50] Vinod Varma Vegesna (2015). “Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security,” International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[51] Chen D, Zhao H. Data security and privacy protection issues in cloud computing, International conference on computer science and electronics engineering 2012.

[52] Miller CD. Associate in AMI- partners. Security in the cloud: concern/excitement?, on July 10th. 2012.

[53] Wueest C, Barcena MB, O'Brien L. Mistakes in the Iaas cloud could put your data at risk. 2015.

[54] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst 2012;28:583–92.

[55] Sax R, Reeher J. How to avoid lock-in and ensure data portability in the cloud, 2014.